UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/458,922	12/10/1999	MOHAMMAD PEYRAVIAN	P-4541.003	9481

7590 11/05/2003

IBM CORPORATION DEPT T81/062
3039 CORNWALLIS ROAD
RTP, NC 27709

EXAMINER	
WU, ALLEN S	

ART UNIT	PAPER NUMBER
2131	7

DATE MAILED: 11/05/2003

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/458,922	PEYRAVIAN ET AL.	
	Examiner	Art Unit	
	Allen S. Wu	2131	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
- Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *07 February 2000* .

2a)☒ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-30* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-30* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *10 December 1999* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

11)☐ The proposed drawing correction filed on _____ is: a)☐ approved b)☐ disapproved by the Examiner.

If approved, corrected drawings are required in reply to this Office action.

12)☐ The oath or declaration is objected to by the Examiner.

Priority under 35 U.S.C. §§ 119 and 120

13)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____ .

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

14)☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. § 119(e) (to a provisional application).

a) ☐ The translation of the foreign language provisional application has been received.

15)☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. §§ 120 and/or 121.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449) Paper No(s) *5* .
4) ☐ Interview Summary (PTO-413) Paper No(s). _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: .

DETAILED ACTION

Claim Rejections - 35 USC § 102

1. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

2. Claims 13-18 are rejected under 35 U.S.C. 102(b) as being anticipated by Haber et al, US Patent 5,136,647.

As per claim 13, Haber et al discloses method for time stamping a document (col 2, ln 33-49) comprising: creating a time stamp receipt including identifying data associated with said document and a time indication (the TSA then prepares the receipt for document, col 6 ln 16-24); transmitting said time stamp receipt to an outside agency (transmittal may be directly to the author or by way of the administrative TSA, col 5 ln 1-16); and cryptographically binding (applying the agency's cryptographic signature scheme, col 2 ln 66-67 and col 3 ln 1-5) at said outside agency said identifying data (digital document, col 2 ln 61-66) and said time indication (adding digital data signifying the current time).

As per claim 14, Haber et al further discloses the identifying data comprising a digital representation of at least a portion of said document (convert the digital document string to a unique number; col 3 ln 6-24; document is hashed, col 6 ln 1-15).

As per claim 15, Haber et al further discloses identifying data comprising a digital sequence derived by application of a deterministic function to at least a portion of said document (reduced digital size by means of a deterministic function, col 3 ln 6-24).

As per claim 16, Haber et al further discloses digital sequence is a hash value derived by application of a one-way hashing function to at least a portion of said document (reduced digital size by means of a deterministic function which may, for example, be any one of a number of algorithms known in the art as "oneway hash functions", col 3 ln 6-24; document is hashed, col 6 ln 1-15).

As per claim 17, Haber et al further discloses the time stamp receipt further including an identification number associated with the document originator (the author whose system identification number is 172 in a 1000 member author universe, col 6 ln 8-15).

As per claim 18, Haber et al further discloses the time stamp receipt further including a sequential record number (TSA generates a time stamp receipt which includes, for example, a sequential receipt number, col 4 ln 3-33).

Claim Rejections - 35 USC § 103

1. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

2. Claims 1-9, 12, 19-27 and 30 are rejected under 35 U.S.C. 103(a) as being unpatentable over Haber et al, US Patent 5,136,647, in view of Takura et al.

As per claims 1 and 19, Haber et al, discloses a method for time stamping a document (col 2, ln 33-49) comprising of a time stamp receipt (certificate, col 3 ln 1-5) including identifying data associated with the document (identity of the author, col 4 ln 3-33) and a time indication (current time, col 4 ln 3-33); binding at said outside agency said identifying data (digital document, col 2 ln 61-66) and said time indication (adding digital data signifying the current time) using a cryptographic binding

scheme (applying the agency's cryptographic signature scheme, col 2 ln 66-67 and col 3 ln 1-5).

Furthermore, Haber et al teaches the binding of the information as described above and the outside agency being able to obtain the current time (adding digital data signifying the current time, col 2 ln 59-66). However, Haber et al does not teach validating the time stamp receipt by comparing the time indication in said time stamp receipt to the current time before binding the information. However, Takura et al, teaches validating the time stamp receipt by comparing the time indication on the time stamp receipt to the current time (checks the time associated with the request by comparing the current time, page 88). Comparing the time indication in the time stamp receipt with the current time is comparing a form of digital data, which is well known in the art. It would have been obvious to one of ordinary skill in the art at the time of the applicant's invention to combine the teachings of Takura et al within the teachings of Haber et al because it would have added validity to the binding of the time stamp receipt information. Binding the time stamp receipt information authenticates the time stamp receipt with the outside agency. Verifying that the time stamp receipt is valid before binding will add the to correctness of the time stamping authority.

In further regards to claim 1, Haber et al further teaches receiving a digital document, (col 2 ln 61-66) at an outside agency (TSA col 2 ln 61-66). Haber et al does not teach the outside agency receiving a time stamp

receipt. However, Takura et al teaches receiving a time stamp receipt at different servers (forwards a copy of the request to each sign server with the time, page 88). Both the digital document and the time stamp receipt consist of digital data. The outside agency, being able to receive a type of digital data, could accept and process a time stamp receipt with methods well known in the art. It would have been obvious to one of ordinary skill in the art at the time of the applicant's invention to combine the teachings of Takura et al within the system of Haber et al because it would have given the outside agency more information on the time exact time the document was created. Providing a time indication in addition to the digital document, in the form of a time receipt, gives the outside agency additional information to conclude the most accurate time the document was created and not just when the document was received by the agency.

In further regard to claims 19, Haber et al teaches creating a time stamp receipt including identifying data associated with said document and a time indication (the TSA then prepares the receipt for document, col 6 ln 16-24) and transmitting said time stamp receipt to an outside agency (transmittal may be directly to the author or by way of the administrative TSA, col 5 ln 1-16).

As per claims 2 and 20, Haber et al further discloses transmitting said binding information to a designated party (transmits the certificate back to the author or by way of the administrative, col 5 ln 4-16).

As per claims 3 and 21, Haber et al further discloses the identifying data comprising a digital representation of at least a portion of said document (convert the digital document string to a unique number; col 3 ln 6-24; document is hashed, col 6 ln 1-15).

As per claims 4 and 22, Haber et al further discloses identifying data comprising a digital sequence derived by application of a deterministic function to at least a portion of said document (reduced digital size by means of a deterministic function, col 3 ln 6-24).

As per claims 5 and 23, Haber et al further discloses digital sequence is a hash value derived by application of a one-way hashing function to at least a portion of said document (reduced digital size by means of a deterministic function which may, for example, be any one of a number of algorithms known in the art as "oneway hash functions", col 3 ln 6-24; document is hashed, col 6 ln 1-15).

As per claims 6 and 24, Haber et al further discloses the time stamp receipt further including an identification number associated with the document originator (the author whose system identification number is 172 in a 1000 member author universe, col 6 ln 8-15).

As per claims 7 and 25, Haber et al further discloses the time stamp receipt further including a sequential record number (TSA generates a time stamp receipt which includes, for example, a sequential receipt number, col 4 ln 3-33).

As per claims 8 and 26,Haber et al further disclose the step of validating said time stamp receipt includes comparing (comparison of a number, col 4 ln 3-33), said identification number (author, A_k, col 4 ln 3-33) and sequential record number (TSA generates a time stamp receipt which includes, for example, a sequential receipt number, col 4 ln 3-33) with data maintained by the outside agency (comparison of a number of relevant distributed certificates, col 3 ln 3-33).

As per claims 9 and 27, Haber et al further discloses said binding step including the signing of a combination of said identifying data and said time indication using a digital cryptographic signature scheme (certifies the resulting separate time-stamped receipt with its own verifiable cryptographic signature col 5 ln 1-16).

As per claim 12 and 30, Haber et al further discloses binding step including an encryption on a combination of said identifying data and said time indication using a secret key controlled by said outside agency (cryptographic public key scheme to be employed in this example

(generally known in the field as the "RSA", signature scheme), col 6 ln 25-35 and col 7 ln 1-24; Haber et al does not explicitly say the private key is controlled by outside agency. However, the RSA signature scheme is well known in the art to have a public and private key pair. Only the signing party knows the private key. Therefore a secret key controlled by the outside agency is to be inherent to the teachings of Haber et al.)

3. Claims 10 and 28 are rejected under 35 U.S.C. 103(a) as being unpatentable over Haber et al, US Patent 5,136,647, in view of Takura et al as applied to claims 1 and 19 above, and further in view of Schneier.

As per claims 10 and 28, Haber et al discloses binding at said outside agency said identifying data (digital document, col 2 ln 61-66) and said time indication (adding digital data signifying the current time) using a cryptographic binding scheme (applying the agency's cryptographic signature scheme, col 2 ln 66-67 and col 3 ln 1-5

Furthermore, Haber et al teaches a secret key controlled by said outside agency (cryptographic public key scheme to be employed in this example (generally known in the field as the "RSA", signature scheme), col 6 ln 25-35 and col 7 ln 1-24; Haber et al does not explicitly say the private key is controlled by outside agency. However, the RSA signature scheme is well known in the art to have a public and private key pair. Only the signing party knows the private key. Therefore a secret key controlled by the outside agency is to be inherent to the teachings of

Haber et al). However the combination of Haber et al and Takura et al does not teach that the binding step includes computing a message authentication code on a combination of identifying data and said time indication using a secret key controlled by said outside agency. A message authentication code is a key dependent one-way hash function. Schneier teaches the generation of message authentication codes with secret keys (IBC-Hash, page 457-459). Binding information together is a manipulation of digital data to achieve one representation of the combination of data. To compute message authentication code, one manipulates the digital data, through the use of one-way hash functions and keys, in such a way as to develop a representation of the combination of data. It would have been obvious to one of ordinary skill in the art at the time of the applicant's invention to combine the teachings of Schneier within the combination of Haber et al and Takura et al because it would have provided a more secure form of binding information together. Message authentication codes are known to provide authenticity without secrecy since only someone with the identical key can verify the hash.

4. Claims 11 and 29 are rejected under 35 U.S.C. 103(a) as being unpatentable over Haber et al, US Patent 5,136,647, in view of Takura et al as applied to claims 1 and 19 above, and further in view of Levine et al, US Patent 6,393,566.

As per claims 11 and 29, Haber et al discloses binding at said outside agency said identifying data (digital document, col 2 ln 61-66) and said time indication (adding digital data signifying the current time) using a cryptographic binding scheme (applying the agency's cryptographic signature scheme, col 2 ln 66-67 and col 3 ln 1-5). However, the combination of Haber et al and Takura et al does not teach that the binding step includes computing a hash value on a combination of identifying data and said time indication. Levine et al teaches the use of hashing algorithms to bind time indication information and identifying data (col 4 ln 1-8). Binding the identifying data and time indication data is a manipulation of digital data. The use of hash algorithms to produce such a binding of data into a representation is well known in the art. It would have been obvious to one of ordinary skill in the art at the time of the applicant's invention to combine the teachings of Levine et al within the combination of Haber et al and Levine et al because it would have added another way of binding the information for the time stamp receipt. Hash algorithms are well known in the art to produce a secure fingerprint of data. Computing a hash value as part of the binding step increases the security of the time stamp from unwanted activity.

Conclusion

5. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

Haber et al, How To Time-Stamp a Digital Document, disclose how to time stamp a digital document using a hash algorithm.

Stefik et al, US Patent 5,638,443, discloses validating the time stamp receipt with the current time.

Blandford, US Patent 5,189,700, discloses binding the identifying data and time indication data by encryption.

Nissl et al, US Patent 6,530,023, disclose validating the time before time with another time source before time stamping the document.

Bergadano et al, US Patent 6,574,627, discloses the generation of message authentication codes with secret keys.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Allen S. Wu whose telephone number is 703-305-0708. The examiner can normally be reached on Monday-Friday 9am-5pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on 703-305-9648. The fax phone number for the organization where this application or proceeding is assigned is (703) 872-9306.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is 703-305-0900.

Allen S. Wu
Examiner
Art Unit 2131

ASW

AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100